IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SSL SERVICES, LLC, Plaintiff,	§ §	
v.	§ §	CIVIL ACTION NO. 2-08-cv-158-TJW
CITRIX SYSTEMS, INC., and CITRIX ONLINE, LLC, Defendants.	§ § § §	

MEMORANDUM OPINION AND ORDER

I. INTRODUCTION

Plaintiff SSL Services, LLC ("Plaintiff") filed suit on April 11, 2008, alleging that Defendants Citrix Systems, Inc., and Citrix Online, LLC (collectively, "Defendants") infringe Plaintiff's U.S. Pat. Nos. 6,061,796 ("the '796 patent") and 6,158,011 ("the '011 patent"). On May 18, 2011, the Court held a claim construction hearing where the parties presented oral arguments regarding the disputed terms. This order will first briefly address the technology at issue in the case and then turn to the merits of the claim construction issues.

II. BACKGROUND OF THE TECHNOLOGY

Generally speaking, the '796 and '011 patents are directed to computer networks known as virtual private networks. "A virtual private network (VPN) is a system for securing communications between computers over an open network such as the Internet." '796 patent, 1:14-16. The '796 and '011 patents claim methods and systems for securely transmitting files from one computer to the other over publicly accessible networks such as the Internet. The asserted claims are claim 27 of the '796 patent and claims 2, 4 and 7 of the '011 patent.

The claimed methods and systems require an authentication and encryption program as

part of their security protocol. The claims require that computer files are encrypted using a "session key" before they are transmitted over the Internet. The encrypted files can be sent securely over the public Internet to another computer because the files are unintelligible until they are decrypted. In order to decrypt the files, the receiving computer must have the same session key as the sending computer.

Using claim 27 of the '796 patent as an exemplary claim, the claimed method allows one client computer to send encrypted files to a second client computer over a "multi-tier virtual private network." The patent refers to the direct communications between the two client computers as peer-to-peer communications. Abstract, Figs. 1A, 1B and 6, 1:27-53. The two client computers communicate with a server to generate and recreate the session key. As shown in Figures 3-4 and 6, the claimed VPN includes "a plurality of client computers," and "a server," each of which has the ability to communicate over the Internet. In Figure 6, client computers are labeled "SmartGATE VPN Client" and the server is labeled "SmartGATE VPN Server." Each client computer contains "client authentication software," "shims" (shown in Figs. 3-4), and "applications with communications capabilities," (labeled "Apps" and "Peer-to-Peer App"). The claim method starts when an application running on a first client computer attempts to open a communication link to a second client computer by making "function calls and requests for service" to "a lower level set of communications drivers." These communications drivers are software on the first client computer that allows the computer to open the communication link. *See* Figs. 2-4. Before the communications drivers can execute the function call, the function call is intercepted by a different software module on the first client computer. The software that intercepts the function call is a "shim." *See, e.g.,* 6:35-59, 6:66-7:6, 8:23-32, 9:42-49, 10:66-11:14, Figs. 2-4. The interception of the function call causes "an applications level

authentication and encryption program" in the first client computer to communicate with the Server and generate a session key. Fig. 3 *see, e.g., also* 9:42-52 (The shim intercepts a function call and "in response thereto" the "authentication client software initiate[s] communications with the authentication server"); 9:53-59; ("session keys generated during the initial communications with the authentication server"); 11:23-27 ("the invention provides for the function calls . . . to be intercepted and the initialization procedure routed through channel 61 to the authentication server"). In Figure 6, the session key generation occurs over communications link 60. 11:21-23. Since the claimed method involves communications between two client computers, the second client computer needs to have the same session key as the first client computer so that it can decrypt the encrypted files sent to it by the first computer. Accordingly, the shim on the first computer also intercepts the address of the second computer, and transmits it to the Server. 9:62-67 ("the principal function of shim 50 is to arrange for the destination of [sic] address of the communication to be supplied to . . . authentication server").

After receiving the address of the second client computer, the Server communicates with the second client computer. 9:60-10:8 ("[t]he latter function provides the authentication server with the client address so that the authentication server can establish a secure and authenticated link with the peer application"). This communication link is shown as 63 in Figure 6. 11:22-36. The Server enables the second client computer to "recreate the session key" that was previously generated in steps. 11:24-37 ("In the case of a peer-to-peer application, in which the clients wish to communicate over a direct link 62 . . . . Server 23 then opens a secured channel 63 . . . and transmits information . . . which allows the client to recreate the channel 60 session key for use in decrypting communications sent over channel 62"). The session key is used by the first client computer to encrypt files, and the encrypted files are then transmitted to the second client

computer. The link between the two client computers is shown as 62 on Figure 6. 11:24-37.

The patents-in-suit share the same abstract that states:

> A virtual private network for communicating between a server and clients over an open network uses an applications level encryption and mutual authentication program and at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computer to intercept function calls, requests for service, or data packets in order to communicate with the server and authenticate the parties to a communication and enable the parties to the communication to establish a common session key. Where the parties to the communication are peer-to-peer applications, the intercepted function calls, requests for service, or data packets include the destination address of the peer application, which is supplied to the server so that the server can authenticate the peer and enable the peer to decrypt further direct peer-to-peer communications

As an exemplary claim of the patents-in-suit, claim 27 of the '796 patent is reproduced below:

> A method of carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising the steps of:
>
> intercepting function calls and requests for service sent by an applications program in one of said client computers to a lower level set of communications drivers;
>
> causing an applications level authentication and encryption program said one of said client computers to communicate with the server, generate a session key, and use the session key generated by the applications level authentication and encryption program to encrypt files sent by the applications program before transmittal over said open network;
>
> intercepting a destination address during initialization of communications between said one of said client computers and a second of said client computers on said virtual private network;
>
> causing said applications level authentication and encryption program to communicate with the server in order to enable the applications level authentication and encryption

program to generate said session key;

transmitting said destination address to said server;

causing said server to communicate with the second of said two client computers;

enabling said second of said two client computers to recreate the session key;

causing said authentication software to encrypt files to be sent to the destination address using the session key; and

transmitting the encrypted files directly to the destination address.

III. GENERAL PRINCIPLES GOVERNING CLAIM CONSTRUCTION

"A claim in a patent provides the metes and bounds of the right which the patent confers on the patentee to exclude others from making, using or selling the protected invention." *Burke, Inc. v. Bruno Indep. Living Aids, Inc.*, 183 F.3d 1334, 1340 (Fed. Cir. 1999). Claim construction is an issue of law for the court to decide. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970-71 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996).

To ascertain the meaning of claims, the Court looks to three primary sources: the claims, the specification, and the prosecution history. *Markman*, 52 F.3d at 979. The specification must contain a written description of the invention that enables one of ordinary skill in the art to make and use the invention. *Id.* A patent's claims must be read in view of the specification, of which they are a part. *Id*. For claim construction purposes, the description may act as a sort of dictionary, which explains the invention and may define terms used in the claims. *Id*. "One purpose for examining the specification is to determine if the patentee has limited the scope of the claims." *Watts v. XL Sys., Inc.*, 232 F.3d 877, 882 (Fed. Cir. 2000).

Nonetheless, it is the function of the claims, not the specification, to set forth the limits of the patentee's invention. Otherwise, there would be no need for claims. *SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). The patentee is free to be his own

lexicographer, but any special definition given to a word must be clearly set forth in the specification. *Intellicall, Inc. v. Phonometrics, Inc.*, 952 F.2d 1384, 1388 (Fed. Cir. 1992). Although the specification may indicate that certain embodiments are preferred, particular embodiments appearing in the specification will not be read into the claims when the claim language is broader than the embodiments. *Electro Med. Sys., S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994).

This Court's claim construction decision must be informed by the Federal Circuit's decision in *Phillips v. AWH Corporation*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). In *Phillips*, the court set forth several guideposts that courts should follow when construing claims. In particular, the court reiterated that "the *claims* of a patent define the invention to which the patentee is entitled the right to exclude." 415 F.3d at 1312 (emphasis added) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To that end, the words used in a claim are generally given their ordinary and customary meaning. *Id*. The ordinary and customary meaning of a claim term "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id*. at 1313. This principle of patent law flows naturally from the recognition that inventors are usually persons who are skilled in the field of the invention and that patents are addressed to and intended to be read by others skilled in the particular art. *Id*.

The primacy of claim terms notwithstanding, *Phillips* made clear that "the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id*. Although the claims themselves may provide guidance as to the meaning of

particular terms, those terms are part of "a fully integrated written instrument." *Id*. at 1315, *quoting Markman*, 52 F.3d at 978. Thus, the *Phillips* court emphasized the specification as being the primary basis for construing the claims. *Id*. at 1314-17. As the Supreme Court stated long ago, "in case of doubt or ambiguity it is proper in all cases to refer back to the descriptive portions of the specification to aid in solving the doubt or in ascertaining the true intent and meaning of the language employed in the claims." *Bates v. Coe*, 98 U.S. 31, 38 (1878). In addressing the role of the specification, the *Phillips* court quoted with approval its earlier observations from *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998):

> Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction.

Phillips, 415 F.3d at 1316. Consequently, *Phillips* emphasized the important role the specification plays in the claim construction process.

The prosecution history also continues to play an important role in claim interpretation. Like the specification, the prosecution history helps to demonstrate how the inventor and the PTO understood the patent. *Id.* at 1317. Because the file history, however, "represents an ongoing negotiation between the PTO and the applicant," it may lack the clarity of the specification and thus be less useful in claim construction proceedings. *Id*. Nevertheless, the prosecution history is intrinsic evidence that is relevant to the determination of how the inventor understood the invention and whether the inventor limited the invention during prosecution by narrowing the scope of the claims. *Id.*

Phillips rejected any claim construction approach that sacrificed the intrinsic record in

favor of extrinsic evidence, such as dictionary definitions or expert testimony. The *en banc* court condemned the suggestion made by *Texas Digital Systems, Inc. v. Telegenix, Inc.*, 308 F.3d 1193 (Fed. Cir. 2002), that a court should discern the ordinary meaning of the claim terms (through dictionaries or otherwise) before resorting to the specification for certain limited purposes. *Phillips*, 415 F.3d at 1319-24. The approach suggested by *Texas Digital*—the assignment of a limited role to the specification—was rejected as inconsistent with decisions holding the specification to be the best guide to the meaning of a disputed term. *Id*. at 1320-21. According to *Phillips*, reliance on dictionary definitions at the expense of the specification had the effect of "focus[ing] the inquiry on the abstract meaning of words rather than on the meaning of claim terms within the context of the patent." *Id*. at 1321. *Phillips* emphasized that the patent system is based on the proposition that the claims cover only the invented subject matter. *Id.* What is described in the claims flows from the statutory requirement imposed on the patentee to describe and particularly claim what he or she has invented. *Id*. The definitions found in dictionaries, however, often flow from the editors' objective of assembling all of the possible definitions for a word. *Id*. at 1321-22.

Phillips does not preclude all uses of dictionaries in claim construction proceedings. Instead, the court assigned dictionaries a role subordinate to the intrinsic record. In doing so, the court emphasized that claim construction issues are not resolved by any magic formula. The court did not impose any particular sequence of steps for a court to follow when it considers disputed claim language. *Id*. at 1323-25. Rather, *Phillips* held that a court must attach the appropriate weight to the intrinsic sources offered in support of a proposed claim construction, bearing in mind the general rule that the claims measure the scope of the patent grant. Having read the parties' papers and carefully considered their arguments and the relevant legal authority,

the Court hereby rules as follows

IV. AGREED CONSTRUCTIONS

Based upon the joint submission of claim construction charts and subsequent arguments in briefing and at the hearing, the following terms of the patent have been agreed to by the parties.

1. "Multi-tier"

Claim language	Agreed Construction
"Multi-tier"	"more than one level or layer"

The term "multi-tier" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the term is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

2. "virtual private network"

Claim language	Agreed Construction
"virtual private network"	"a system for securing communications between computers over an open network"

The phrase "virtual private network" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the phrase is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

3. "server"

Claim language	Agreed Construction
"server"	"software running on a computer that provides services to client computers"

The term "server" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the term is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

4. "plurality"

Claim language	Agreed Construction
"plurality"	"more than one"

The term "plurality" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the term is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

5. "lower level set of communications drivers"

Claim language	Agreed Construction
"lower level set of communications drivers"	"set of communications drivers below the applications layer"

The phrase "lower level set of communications drivers" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the phrase is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

6. "session key"

Claim language	Agreed Construction
"session key"	"a sequence of bits that is input into an encryption algorithm to encrypt data for a session"

The phrase "session key" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the phrase is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

7. "generate a session key"

Claim language	Agreed Construction
"generate a session key"	"to produce a session key"

The phrase "generate a session key" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the phrase is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

8. "encrypt"

Claim language	Agreed Construction
"encrypt"	"to render unintelligible without decrypting"

The term "encrypt" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. A review of the intrinsic evidence confirms that the parties agreed construction is consistent with how the term is used in the claims and the specification. Thus, the Court adopts the parties' agreed construction.

V. TERMS IN DISPUTE OF THE PATENTS-IN-SUIT

1. The Preambles of the Asserted Claims (Claim 27 of the '796 Patent and Claims 4 and 7 of the '011 Patent) are Limitations of the Claims

An initial threshold question is whether the preambles of claim 27 of the '796 patent and claims 4 and 7 of the '011 patent are limitations of the claims. "In general, a preamble limits the invention if it recites essential structure or steps, or if it is 'necessary to give life, meaning, and vitality' to the claim." *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (quoting *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999)). "Conversely, a preamble is not limiting 'where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention.'" *Id.* (quoting *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir. 1997)). Similar to other issues in the patent law arena, there is not a well defined litmus test to determine when a preamble limits claim scope. *Corning Glass Works v. Sumitomo Electric U.S.A., Inc.*, 868 F.2d 1251, 1257 (Fed. Cir. 1989). With these principals in mind, the Court turns to the claim language to determine if the preambles provide further limitation of the claims.

Plaintiff argues that the preambles of the asserted claims do not further limit the claims because the bodies of the asserted claims provide ample context for understanding the meaning of every recited term. Defendants respond that the preambles are limiting because they contain terms that provide "the only antecedent basis" for terms appearing in the body of the claim. To support their argument, Defendants rely on *Seachange Int'l, Inc. v. C-Cor Inc.*, 413 F.3d 1361, 1376 (Fed. Cir. 2005). In *Seachange*, the court found that the preamble provided the only antecedent basis and thus the context essential to understand the meaning of the term. *Id.* at 1376. In the present case, the preamble of claim 27 of the '796 patent provides the only antecedent basis for the terms: "multi-tier virtual private network," "server," and "plurality of

client computers." Similarly, the preambles of claims 4 and 7 of the '011 patent provide the only antecedent basis for the terms: "server," "client computer," "function calls and requests for service," "lower level set of communications drivers," and "open network." As the court stated in *Catalina*, "dependence on a particular disputed preamble phrase for antecedent basis may limit claim scope because it indicates a reliance on both the preamble and claim body to define the claimed invention." *Catalina*, 289 F.3d at 808. Accordingly, the Court concludes that the preambles are limiting because the body of the claims rely on the preamble to provide proper antecedent basis for terms appearing in the body of the claims, as well the context in which the claimed invention is implemented. In other words, the preambles provide more than a stated purpose or intended use for the invention.

2. The Steps of the Asserted Method Claims (Claim 27 of the '796 patent and Claim 7 of the '011 patent) are not Required to be Performed in the Exact Order Recited in the Claim Language, but the Steps are Required to be Performed in a High-Level Logical Grouping

A second threshold question is whether the steps recited in method claim 27 of the '796 patent and method claim 7 of the '011 patent must be performed in their recited order. As a general rule, method claim steps are not construed to require a specific order. *Interactive Gift Express, Inc. v. CompuServe Inc.*, 256 F.3d 1323, 1342 (Fed. Cir. 2000). Exceptions to this rule occur only if the steps actually recite or require, via grammar or logic, a specific order, or if the specification "directly or implicitly requires such a narrow construction." *Altiris, Inc., v. Symantec Corp*., 318 F.3d 1363, 1369-70 (Fed. Cir. 2003) (quoting *Interactive Gift*, 256 F.3d at 1342-43). In their brief, Defendants contend that the steps must be performed in exactly the order recited in the claim. Plaintiff disagrees. During the hearing, both parties retreated from their absolute positions and conceded that the claim language does require that certain steps must be performed in a logical order. Notwithstanding, Plaintiff argued that it should be left to the

jury to determine what those certain steps are and what logical order they should be performed in. The Court disagrees.

In the present case, the stated objectives of the claimed invention require that a number of the steps must occur in a specific order. Otherwise, the claimed invention would not operate in a manner that would accomplish the stated principal objective of authenticated secure peer-to-peer communications. '796 patent, 5:66-6:4. The Court first notes that Figure 7 illustrates a high-level order that must be followed for the claimed invention to meet its principal objective. Figure 7 illustrates communications directly with the application level portion of the server, steps 100-103, as well as peer-to-peer communications, steps 104-109. '796 patent, 11:59-64. The specification further notes that a number of steps 104-109 are included in steps 100-103. '796 patent, 12:11-19. With this in mind, the Court observes that at a high level there are basically four ordered steps in the claimed invention. First, the connection request and destination address is intercepted. Second, communication is established with the authentication server and a session key is generated. Third, a communication channel is established between the server and the destination client. Finally, the destination client is able to decrypt and encrypt files.

Applying this general outline to claim 27, the Court finds that the steps of "intercepting function calls and requests for service sent by an applications program in one of said client computers to a lower level set of communications drivers" and "intercepting a destination address during initialization of communications between said one of said client computers and a second of said client computers on said virtual private network" must precede all other steps. These steps, however, are not required to occur in the order listed here or in the order that they are recited in the claims. The only requirement is that both steps occur before any subsequent steps. This first group of steps is then followed by the steps of "causing an applications level

authentication and encryption program said one of said client computers to communicate with the server, generate a session key, and use the session key generated by the applications level authentication and encryption program to encrypt files sent by the applications program before transmittal over said open network," "causing an applications level authentication and encryption program said one of said client computers to communicate with the server, generate a session key, and use the session key generated by the applications level authentication and encryption program to encrypt files sent by the applications program before transmittal over said open network," and "transmitting said destination address to said server," Again, these steps will follow the first group of steps and precede the subsequent group of steps, but not necessarily in the order listed here or in the order they are recited in the claims. The first and second groups of steps are then followed by the step of "causing said server to communicate with the second of said two client computers." This is the third group of steps. Finally, the first, second, and third groups of steps are then followed by the steps of "enabling said second of said two client computers to recreate the session key," "causing said authentication software to encrypt files to be sent to the destination address using the session key," and "transmitting the encrypted files directly to the destination address." Again, these steps are not required to occur in the order listed here or in the order that they are recited in the claims, the only requirement is that they occur after all of the steps included in the first, second, and third group.

Given that the '796 patent and '011 patent share a common specification, the Court finds that this general outline for the required order steps is directly applicable to claim 7 of the '011 patent. In addition, the Court finds that this order does not exclude any of the preferred embodiments. For example, it does not require multiple acts of communicating between an applications level encryption program and a server during initialization of communications

between a client computer and a server. It also does not require the session key to be generated before a destination address is intercepted. Accordingly, the Court concludes that the steps recited in method claims 27 of the '796 patent and 7 of the '011 patent must be performed in the logical order discussed above.

3. "client computer"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
client computer	A user of a computer or the computer itself that request data or services from a server	A computer that uses the services provided by a server

The Court construes "client computer" as "a computer that request data or services from a server."

A. Parties' Construction Arguments

The parties dispute whether the phrase "client computer" was intended to refer solely to computer hardware, or also as a synonym for the user of the computer. Plaintiff argues that the patentee did not intend to limit the term "client computer" to the computer itself. Defendants contend that the intrinsic evidence is clear that a "client computer" is a computer, not a person. Given this, the Court turns to the intrinsic evidence to determine how one of ordinary skill in the art would interpret this phrase.

B. Findings

To begin its analysis, the Court first turns to the language of the claims, as it provides "substantial guidance as to the meaning of particular claim terms." *Phillips*, 415 F.3d at 1313 (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). The phrase "client computer" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011

patent. Two things are evident from the claim language. First, the phrase is used consistently in each patent and is meant to have a similar meaning. Second, the claim language indicates that a "client computer" is a computer, and not simply a user of the computer as Plaintiff argues. For example, claim 4 of the '011 patent is directed solely to "[c]omputer software for installation on a client computer." Claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent all require "client computers each including means for transmitting data to and receiving data from an open network," and client computers containing "applications level" software. Thus, the claim language itself indicates that a "client computer" is actually a computer, and not the user of the computer.

The Court next turns to the specification as it "is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." *Id.* at 1315 (citation omitted). The specification likewise indicates that "a client computer" is a computer. *See, e.g.,* 11:1-7 ("The principal components of the overall system are the client computers containing software of the type illustrated in FIGS 2-5…"); 1:43-44 ("applications on the client computers"); 6:40-42 ("network interface layers of a client computers communications hierarchy"). The Court agrees with Defendants that there is not a single recitation of the term "client computer" in the patents that suggests that a client computer is anything other than a computer. One of ordinary skill in the art would not understand a computer user to be a computer containing software or applications, or have the network interface layers described in the patent.

In an attempt to avoid this intrinsic evidence, Plaintiff argues that the details of the inner workings of the "authentication" process are described in detail in U.S. Patent No. 5,602,918 ("the '918 patent"), which was incorporated by reference into the '796 patent specification. '796

patent, 2:28-32. Specifically, Plaintiff contends that in the '918 patent, an "authentication" procedure is described which requires a user to provide identifying information (e.g., "unique user ID") for the purposes of authenticating communications between one party in the form of a "gateway processor" and another party in the form of a "client." Although this may be true, it is of little relevance to the phrase "client computer" as the phrase is used in the '796 and '011 patents. Again, the disputed phrase is "client computer," not just "client." Importantly, the phrase "client computer" does not appear anywhere in either the claims or the specification of the '918 patent. In stark contrast, the disputed phrase "client computer" appears numerous times in the '796 and '011 patent claims and specification. Thus, the use of the term "client" in the '918 patent carries very little weight.

Moreover, even when the term "client" appears in the '796 patent, it is describing computers or "clients" that are "are equipped with an applications level encryption and mutual authentication program which includes at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computers communications hierarchy." '796 patent, 6:35-42. The patent confirms that the recited programs are not installed on users, they are installed on computers. Accordingly, consistent with its use in the '796 and '011 patent, the Court construes the phrase "client computer" as "a computer that request data or services from a server."

4. "means for transmitting data to and receiving data from an open network"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
means for transmitting data to and receiving data from an open network	For claim 27 of the '796 Patent, the clause should not be construed pursuant to 35 U.S.C. § 112, ¶ 6. However, if the Court decides the clause needs to be construed pursuant to § 112, ¶ 6, the claimed functions of "transmitting data to and receiving data from an open network" is performed by the following corresponding structure in the specification of the '796 Patent (and equivalents thereof): at least lower level communication drivers and hardware (e.g., a network or modem connection). For the claims of the '011 Patent, § 112, ¶ 6 does not apply, at least with respect to the client computer, recited in claims 2, 4, and 7, because these claims specifically recite the structure used to perform the claimed functions of "transmitting data to and receiving data from an open network." Moreover, the "means" limitations in claims 4 and 7 are recited in the preamble of the claims, which is not a limitation to the claimed invention. However, if the Court decides the clause needs to be construed pursuant to § 112, ¶ 6, the claimed functions of "transmitting data to and receiving data from an open network" is performed by the following corresponding structure in the specification of the '011 Patent (and equivalents): at least lower level communication drivers and hardware (e.g., a network or modem connection).	This element is governed by 35 U.S.C. § 112(6). Structure: TDI layer, NDIS layer, physical layer, and may or may not include sockets and disclosed communications protocols Function: transmitting data to and receiving data from an open network

The Court finds that the phrase "means for transmitting data to and receiving data from an open network" should be construed pursuant to 35 U.S.C. § 112, ¶ 6 for claim 27 of the '796 patent. The Court finds that the recited function is transmitting data to and receiving data from an open network. The corresponding structure that corresponds to the means is the lower level communications drivers and hardware (such as a network or modem connection) described in the

specification or equivalents thereof. For claims 2, 4 and 7 of the '011 patent, the Court finds that the claims do not need to be construed as a "means-plus-function" element because the claims recite sufficient structure to perform the claimed function in its entirety.

A. Parties' Construction Arguments

The parties dispute whether the phrase should be construed as a "means-plus-function" element pursuant to 35 U.S.C. § 112, ¶ 6. Plaintiff contends that the phrase is included in the preamble and is not a limitation of the claims. Defendants contend that the preamble is a limitation of the claims and that the term should be construed pursuant to 35 U.S.C. § 112, ¶ 6. Because the Court has determined that the preamble is a limitation of the claims, the Court will construe the disputed phrase for claim 27 of the '796 patent.

B. Findings

A claim limitation that "contains the word 'means' and recites a function is presumed to be drafted in means-plus-function format under 35 U.S.C. § 112, ¶ 6." *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1366 (Fed. Cir. 2008). This presumption can be rebutted if the claim limitation itself recites sufficient structure to perform the claimed function in its entirety. *TI Grp. Auto. Sys.'s (N. Am.), Inc. v. VDO N. Am., L.L.C.*, 375 F.3d 1126, 1135 (Fed. Cir. 2004) (holding that the term "pumping means" in a patent directed to fuel pump assembly technology was not a means-plus-function limitation as the limitation recited not only a pumping means, but its structure, location, and operation). The Court first finds that claim 27 of '796 does not recite sufficient structure to perform the claimed function in its entirety, thus Plaintiff has failed to rebut the presumption that the claim was drafted in means-plus-function format. As stated in the claim and agreed to by the parties, the Court finds that the recited function is "transmitting data to and receiving data from an open network." The Court further finds that the corresponding

structure for performing the recited function is taught in the specification as being one or more of the disclosed communications layers and the related hardware. For example, these communication layers include TDI layer 21, socket layer 22, hardware driver layer 24, and/or network connections. '796 patent, 8:35-55. Defendants do not dispute that these layers are the corresponding structure, and only contend that the structure may or may not include communications protocols. The Court disagrees with this proposition. Accordingly, the Court finds that the corresponding structure is the lower level communications drivers and hardware (such as a network or modem connection) described in the specification or equivalents thereof.

Regarding claims 2, 4 and 7 of the '011 patent, the Court finds that the claims do not need to be construed as a "means-plus-function" element because the claims recite sufficient structure to perform the claimed function in its entirety. For example, claim 2 recites "wherein said means. . . includes . . . applications level encryption and authentication software . . . ; at least one lower level set of communications driver; and a shim." Similarly, claims 4 and 7 recite "wherein said means . . . includes a lower set of communications drivers, said lower set of communications drivers being arranged to receive function calls and requests for service from an applications program in order to transmit and receive said data." Accordingly, as it applies to claims 2, 4 and 7 of the '011 patent, Plaintiff has rebutted the presumption that the claim was intended to be drafted in means-plus-function format. Indeed, the claims explicitly recite the lower level communications driver.

5. "intercepting function calls and requests for service"/"intercept function calls and requests for service"/"intercepting said function calls and requests for service"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
intercepting function calls and requests for service intercept function calls and requests for service intercepting said function calls and requests for service	"intercepting" and "intercept" means receiving from a software module that which concerns another software module. "function calls and requests for service" means request for a desired function, service, operation or event.	Seizing by a shim an applications program's function calls and requests for service intended for another software module "function call" means "A call from a program that passes control to another software routine" "request for services" means "A request from a program that passes control to another software routine"

The Court construes "intercepting function calls and requests for service" as "using a shim to intercept or divert a request for a desired function, service, operation or event."

A. Parties' Construction Arguments

The parties dispute whether the term "intercept" in the disputed phrase should be construed to mean "receiving," as proposed by Plaintiff, or "seizing by a shim," as proposed by Defendants. The parties also dispute the construction of the phrase "calls and request service." Plaintiff contends that it means "request for a desired function, service, operation or event." Defendants argue that "function call" means "a call from a program that passes control to another software routine," and "request for services" means "a request from a program that passes control to another software routine." The Court notes that based on their proposed constructions, Defendant agree that a "function call" or "request for services" is a request or call from a program. For the following reasons, the Court does not adopt either party's proposed construction.

B. Findings

To begin its analysis, the Court first turns to the claims themselves. The phrases "intercepting function calls and requests for service" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. The Court concludes that the phrases are used consistently in each patent and are meant to have a similar meaning. The Court also concludes that the claim language indicates that intercepting is the same as diverting, and that the intercepting and diverting occurs by using a shim. Specifically, claim 27 associates "intercepting function calls and requests for service sent by an applications program" with "intercepting a destination address during initialization of communications." That is, like the recited function calls and request for services, the destination address is also intercepted. Claim 19, further recites that "wherein a peer application destination address, included in said *intercepted* requests for service, is *diverted* by the transport driver interface layer shim and supplied to the server during communications with the server." Likewise, claim 15 also recites "wherein a peer application destination address, included in said function calls to the socket, is *diverted* by the socket shim, and wherein a destination address including said *intercepted* function calls is supplied to the server during communications with the server." Similarly, claim 8 recites "wherein a peer application destination address, included in said *intercepted* requests for service, is *diverted* by the transport driver interface layer shim and supplied to the server during communications with the server." Thus, the claims of the '796 patent explicitly recognize that intercepting function calls and requests for service includes diverting the request by using a shim. Accordingly, the claim language does not support Plaintiff's proposed construction of "receiving" because receiving is too broad and does not capture the limitation of proactively diverting a call or request. That is, simply receiving a call or request is not the same as diverting a call or request.

Defendants' proposed construction of "seizing," however, is not supported by the claim language or the intrinsic evidence. Indeed, the call or request is not seized, but instead is diverted or re-routed. During the claim construction hearing, Defendants conceded that "seizing" probably went too far and proposed to stick with the claim language itself and use "intercepting" in the construction.

In opposition to this claim language, Plaintiff contends that the doctrine of claim differentiation indicates a shim is not required to intercept the function calls and requests for service. Specifically, Plaintiff argues that both claim 27 of the '796 patent and claim 7 of the '011 patent purposefully omit the term "shim" from the claim scope. And that claim 28 of the '796 patent, which depends from independent claim 27, explicitly adds that the claimed "intercepting a destination address" function is performed using a "shim." Plaintiff's claim differentiation argument fails, however, because claim 28 is not simply differentiated by its use of the word "shim." Rather, claim 28 further limits the location of the shim. Specifically, claim 28 states that the shim is "positioned between a peer-to-peer applications program and a layer." That is, the location of the shim is not recited in independent claim 27. Moreover, as will be discussed in more detail, the specification only describes using a "shim" to perform the claimed interception, and refer to "shims" as "the invention." Thus, the scope of the claims is limited to interception by a shim as confirmed by the all of the claims, even the ones not asserted. *See, e.g., Versata Software, Inc. v. SAP Am., Inc.*, 2:07-CV-153, 2009 U.S. Dist. LEXIS 45751, at *17-18 (E.D. Tex. May 19, 2009) (Everingham, M.J.) (disregarding plaintiff's claim differentiation argument because the specification limited the scope of the invention). Of course, the scope of this limitation is directly tied to the Court's construction of the disputed term "shim."

Turning to the specification, the Court finds that it further supports construing "intercepting function calls and requests for service" as "using a shim to intercept or divert a request for a desired function, service, operation or event." First, the specification states that the "shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket and, in response thereto, having the authentication client software initiate communications with the authentication server 23, …. Shim 50 also causes files 41 intended for the TDI layer to be diverted to the authentication software for encryption based on the session keys generated during the initial communications with the authentication server…" '796 Patent, 9:47-57. Thus, like the claim language, the specification states that intercepting a call or file is the same a diverting a call or file via a shim.

During the claim construction hearing, Plaintiff argued that because Figure 2 and the related discussion does not disclose the use of a shim, including a shim in the construction would be excluding this embodiment. *See, e.g.,* '796 patent 8:43-49. The problem with Plaintiff's argument is that Figure 2 does not illustrate an embodiment of the claimed invention, but rather illustrates and describes the prior art. Naturally, one would not expect to find the key feature of the invention described as the prior art. The flaw of Plaintiff's argument is that it fails to recognize that Figure 2 is described and labeled "prior art."

More importantly, the use of a shim to intercept function calls and requests for services is repeatedly highlighted throughout the patents as the key feature of the claimed inventions. For example, the patent sets out a list of the objectives of "the invention." 5:66-6:34. The paragraph immediately following explicitly states that the inventions require shims for interception:

> *These objectives of the invention* are accomplished by providing a virtual private network . . . in which the clients are equipped with an applications level encryption and mutual authentication

> program which *includes at least one shim* positioned above either the socket, transport driver interface, or network interface layers of a client computers communications hierarchy, and which *intercepts function calls* or data packets . . .

(6:35-43) (emphasis added). The patent states that the invention itself is the use of shims:

> In addition, it [sic] noted that the client computer architectures illustrated in FIGS. 3-6, which are modified versions of the architecture of FIG. 2, is to be used with an overall network layout such as the one illustrated in FIG 6 . . . *The invention is not merely the addition of shims to the client software, but involves the manner in which the shims are used in the establishment of the authentications and key generation links to the server.*

8:23-32 (emphasis added). Indeed, there is no description of intercepting function calls and requests for service from an applications program to a lower level set of communications drivers other than by using shims. In view of this intrinsic evidence, the Court finds that the scope of the inventions is limited to a "shim." *See Honeywell Int'l, Inc. v. ITT Indus., Inc.*, 452 F.3d 1312, 1318 (Fed. Cir. 2006) (holding that the written description's references to "this invention" or "the present invention," and disclosure of only one embodiment limited the scope of the claims). "The public is entitled to take the patentee[s] at [their] word and the word was that the invention is a [shim]." *Id.*

Finally, the '011 prosecution history confirms that the claimed "interceptor" is a shim. In response to a rejection of all of the claims, including application claim 31 (which issued as claim 7 of the '011 patent), the patentee distinguished the claims over the prior art, stating:

> In other words, instead of just providing a socket that provides encryption services as in the Elgamel patent, *the present invention inserts a shim between the sockets layer and applications programs that use the sockets layer*. The shim *diverts* function calls to an applications level encryption and authentication program in a manner that is transparent to both the socket and the applications program, and the applications level encryption and authentication program initially directs communications to an authentication server in a manner which is also transparent to the

applications program and sockets layer.

Dkt. No. 101-19 at 75 (emphasis added). Thus, the patentee explicitly stated that the present invention includes a shim that is used to divert function calls and request for services. Accordingly, based on the intrinsic evidence, the Court rejects both parties' proposed construction and construes "intercepting function calls and requests for service" as "using a shim to intercept or divert a request for a desired function, service, operation or event."

6. "authentication and encryption program/encryption and authentication software"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
authentication and encryption program/encryption and authentication software	"Authentication and encryption program" - does not need to be construed and should be given its plain and ordinary meaning. However, if the Court determines that the term should be construed, "authentication and encryption program" means program or software that is capable of performing authentication functions, encryption functions, or both depending on the limitations set forth in the claim . "Authentication" does not need to be construed and should be given its plain and ordinary meaning. However, if the Court determines that the term should be construed, "authentication" means the process of verifying or validating. "Encryption" does not need to be construed and should be given its plain and ordinary meaning. However, if the Court determines that the term should be construed, "encryption" means the process of coding or putting into a form that cannot be understood without decoding.	Software that performs authentication and encryption "Authentication" means "The process of verifying the identity of an entity" "Encryption" means "the process of rendering data unintelligible without decrypting" "request for services" means "A request from a program that passes control to another software routine

The Court construes "authentication and encryption program" as "a program that verifies the identity of a client or server and renders data unintelligible without decrypting"

A. Parties' Construction Arguments

The parties dispute whether the claimed program must perform both authentication and encryption, or whether the "program" need only be capable of performing authentication functions, encryption functions, or both depending on the limitations set forth in the claim. Plaintiff argue that the phrases "authentication and encryption" were intended to be used in their ordinary sense as a generic descriptor or label for software that, in various embodiments, can carry out authentication functions, encryption functions, or both. Defendants argue that Plaintiff is attempting to rewrite the claim term to "authentication *or* encryption software." Given this, the Court turns to the intrinsic evidence to determine how one of ordinary skill in the art would interpret this phrase.

B. Findings

To begin its analysis, the Court first turns to the claims themselves. The phrases "authentication and encryption program" and "encryption and authentication software" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. The Court concludes that the phrases are used consistently in each patent and are meant to have a similar meaning. The Court also concludes that the claim language explicitly states that the "authentication and encryption program" and "encryption and authentication software" both authenticates the client computer as well as renders data unintelligible without decrypting. For example, claim 27 states that authentication and encryption program generates a session key that is to encrypt files, as well as cause the server to communicate with the second client computers to verify the identity of the client computer. Likewise, claims 2 and 4 of the '011 patent recite that the encryption and authentication software is arranged to communicate with the server in order to (1) mutually authenticate the server and the client computer initiating communications

with the server and (2) generate a session key for use by the client computer initiating communications to encrypt files. Finally, claim 7 of the '011 patent recites that the authentication and encryption program communicates with the server in response to receiving said intercepted function calls and requests for service by generating a session key and then uses the session key to encrypt file sent by the applications program. Thus, like claim 27, the program establishes communication with a server for authentication and then generates a session key to encrypt the files. Accordingly, the claim language supports Defendants' argument that the claimed program must perform both authentication and encryption.

The Court is not persuaded by Plaintiffs' arguments as they relate to the specification and the prosecution history. Although it is true that the specification does not state that a program having both authentication and encryption functions is an essential component of the invention, the claim language itself forecloses this possibility that the program performs either authentication or encryption. As discussed, the claim language explicitly states that the "authentication and encryption program" and "encryption and authentication software" both authenticates the client computer as well as renders data unintelligible without decrypting. Indeed, claim 27 of the '796 patent explicitly states that the "authentication software" encrypts "files to be sent to the destination address using the session key."

Regarding the term "authentication," the Court notes that neither the claims nor specification of the '796 and '011 patent explicitly define the term. However, in describing the SmartGATE™ system—used in one of the preferred embodiments—the specification discloses an exemplary authentication process where the client software reads a request for communications by an applications program, and then proceeds to establish its own communications link with the destination server to determine if the server is an authentication

server. '796 patent, 4:66-5:8. Specifically, the specification states that "[i]f it is not, control of communications is relinquished, but if it is, then the security program and the server carry out a challenge/response routine in order to generate the session key, and all further communications are encrypted by the security program." *Id.* This exemplary embodiment indicates that authentication is the process of verifying the identity of a client or sever. In addition, the '918 patent, which is incorporated by reference, also indicates that "authentication" is "verification of identity." '918 patent, 3:21-27 ("a method of establishing the identity"); 4:32-42 ("establish to their mutual satisfaction the identity of both the gateway processor and the client"); 5:29-31 ("the illustrated mutual identification procedure allows the gateway processor to verify the legitimacy of the client"); Figs. 3A & 3B. Thus, the Court construes "authentication" as "verifying the identity of a client or server." Given this, and in the light of the parties agreed construction for the term "encrypt," the Court construes "authentication and encryption program" as "a program that verifies the identity of a client or server and renders data unintelligible without decrypting"

7. "encrypt files"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
encrypt files	"files" means a collection or segment of data	"files" means a collection of related data or program records treated as a basic unit of storage

The Court construes "encrypt files" as "to render a set of data used by a program unintelligible without decrypting."

A. Parties' Construction Arguments

The parties agree that "encrypt" means "to render unintelligible without decrypting." The dispute revolves around the term "files." Plaintiff argues that the patentee acted as its own lexicographer and defined the term "files" as a collection or segment of data. Defendants argue

that the term "files" should be given its ordinary meaning, which they contend is "a collection of related data or program records treated as a basic unit of storage." Essentially, the parties dispute whether the phrase "encrypt files" should include encrypting "datagrams" and "packets." Given this, the Court turns to the intrinsic evidence to determine how one of ordinary skill in the art would interpret this phrase.

B. Findings

To begin its analysis, the Court turns to the claims themselves. The term "encrypt files" appears in claim 27 of the '796 patent and claims 2, 4, and 7 of the '011 patent. The Court first concludes that the phrase is used consistently in each patent and is meant to have a similar meaning. Second, the Court concludes that the claim language distinguishes encrypting files from encrypting packets. Specifically, claim 1 of the '796 patent recites "means for causing an applications level authentication and encryption program in said one of said client computers to communicate with the server, generate a session key, and use the session key generated by the applications level authentication and encryption program to *encrypt files* sent by the applications program before transmittal over said open network, and means for intercepting files packaged by a transport driver interface layer to form packets and *encrypting the packets* using a session key generated during communications between corresponding lower layers of the server and said one of said client computers." '796 patent, claim 1. Thus, the explicit claim language indicates that encrypting files is distinct from encrypting packets. In addition, the patent, expressly distinguish between "files" and "packets" and "datagrams." The patents state that datagrams or packets *carry* encrypted files. 8:61-67 ("[I]t is to be understood that *datagrams or packets* 31 *carry* both the communications used to establish the secure channel, and the *encrypted files* subsequently sent therethrough.") (emphasis added). Although the specification discusses encrypting packets

and other data, the claims define the scope of the patent protection and here, the patentee claimed encrypting "files." That is, the term cannot be construed so broadly that it would include "packets," "datagrams" or other types of communications. However, this does not mean that an accused device that encrypts packets automatically falls outside of the scope of the claims, but instead requires that at a minimum the encryption must occur at the file level. To this end, Plaintiff's proposed construction is too broad because it would include any "collection or segment of data," which could include "datagrams" and "packets."

The section of the specification relied upon by Plaintiff to argue that "files" and communications are synonymous is a reference to the prior art (*see* 8:33-34 and Fig. 2 (labeled "prior art")), and states only that "data communications" from an application are encrypted and are "encrypted files" before they ever exit the application layer. *See* 8:56-61 & Fig. 2 (showing encrypted files 35 at the application layer). Again, the described "encrypted files" are at the application layer and this passage is not a reference to encryption of "datagrams" or "packets." As stated in the patent, it is the TDI layer (below the application layer) where datagrams or packets are formed. 8:50-52 ("causing the TDI layer to form datagrams or packets"), Figs. 2-5. Simply stated, "encrypted files" from the application layer are not encrypted datagrams or packets.

Unfortunately, beyond this distinction, the patent does not provide an explicit definition for the term "files." Accordingly, the Court will consider the extrinsic evidence provided by the parties. Defendants provide the Microsoft Press Computer Dictionary (1997) that defines "files," in part, as "a complete, named collection of information, such as a program, a set of data used by a program, or a user-created document." (Dkt. No 101-8 at 6 (Microsoft Press Computer Dictionary (3rd ed. 1997).) The Court finds that a portion of this definition is consistent with the

intrinsic evidence discussed above. Specifically, the Court concludes that one of ordinary skill in the art would interpret "files" as "a set of data used by a program." This is because the claims generally recite that the "authentication and encryption programs … encrypt files sent by the applications programs." Thus, given that the encrypted files are sent by the application programs, the files necessarily are sets of data used by the application programs. Accordingly, the Court construes "encrypt files" as "to render a set of data used by a program unintelligible without decrypting."

8. "destination address"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
destination address	Identifier for a desired location	The network layer identifier of the location on the network of the second client computer, which for Internet communications is the IP address of the second client computer.

The Court construes "destination address" as "the network address of a computer or server."

A. Parties' Construction Arguments

The parties dispute whether the disputed phrase "destination address" simply refers to a "destination," as proposed by Plaintiff, or refers to an address field found in an IP header when using an IP-based protocol to send data over the Internet, as proposed by Defendants. Given this, the Court turns to the intrinsic evidence to determine how one of ordinary skill in the art would interpret this phrase.

B. Findings

To begin its analysis, the Court turns to the claims themselves. The phrase "destination

address" appears in claim 27 of the '796 patent. The Court concludes that the phrase is used consistently through-out the claim. The Court also concludes that the claim language indicates that the phrase "destination address" refers specifically to the address on the network of the claimed second client computer. Specifically, claim 27 claims a method for allowing a first client computer to send encrypted files directly to a second client computer over a network. One step in the process, is "intercepting a *destination address* during initialization of communications between said one of said client computers and *a second of said client computers* on said virtual private network." Moreover, the "destination address" is transmitted to the server so that the server can open a communication link with the second client computer. "Encrypted files" are transmitted directly from the first client computer to the "destination address." The "destination address" is necessarily that of the second client computer. Therefore, the claim language indicates that the "destination address" is the location of the second computer on the network. A review of the specification further confirms this to be true.

Although it is true that references to both "destination" and "destination address" can be found through-out the specification, the Court finds that these terms are not used interchangeably, especially in the light of the claim language. Moreover, to construe "destination address" as simply "destination" would improperly write the term "address" out of the claim. Defendants' proposed construction, however, goes too far and attempts to limit the claimed invention to one disclosed transport protocol. Specifically, Defendants argue that the term "destination address" is used in the patents to refer to an address field found in an IP header when using an IP-based protocol to send data over the Internet. '796 patent, 3:16-28. However, as is stated in the specification, the claimed invention is not limited to IP based protocols and may use non-IP based protocols. *Id.* Thus, Defendants' proposed construction would exclude

embodiments of the invention. Likewise, the Court finds Defendants' argument relating to the Hedrick art cited during the prosecution history unpersuasive. Accordingly, the Court construes "destination address" as "the network address of a computer or server."

9. "intercepting a destination address"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
intercepting a destination address	The term "intercepting a destination address" do not need to be construed, as the terms "intercepting" and "destination address" are discussed elsewhere in this chart. However, if the Court determines that the terms should be construed, the terms "intercepting a destination address" mean receiving an identifier for a desired location	Seizing by a shim a destination address

For the reasons stated above relating to the disputed term "intercepting," as it is used in the disputed phrase "intercepting function calls and requests for service," and the disputed phrase "destination address," the Court construes "intercepting a destination address" as "using a shim to intercept or divert the network address of a computer or server." Indeed, the parties did not provide any new arguments as it relates to this disputed phrase, but instead relied on the arguments presented for the disputed phrase "intercepting function calls and requests for service" and "destination address." As discussed above for both of these disputed phrases, the Court's construction is grounded in the intrinsic evidence. For example, Claim 19 recites that "wherein a peer application *destination address*, included in said *intercepted* requests for service, is *diverted* by the transport driver interface layer shim and supplied to the server during communications with the server." Thus, the claim language explicitly states that intercepting a destination address include using a shim to divert the destination address.

10. "causing said applications level authentication and encryption program to communicate with the server in order to enable the applications level authentication and encryption program to generate said session key"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
causing said applications level authentication and encryption program to communicate with the server in order to enable the applications level authentication and encryption program to generate said session key	The clause "causing said applications level authentication and encryption program to communicate with the server in order to enable the applications level authentication and encryption program to generate said session key" does not need to be construed and should be given its plain and ordinary meaning. However, if the Court decides the clause needs to be construed, the construction of the clause "causing said applications level authentication and encryption program to communicate with the server in order to enable the applications level authentication and encryption program to generate said session key" may be derived from the terms already construed in this chart (i.e., "applications level authentication and encryption program," "the server" and "session key").	The applications level authentication and encryption program in the first client computer produces the session key through communications with the server

After reviewing the disputed phrase in the context of the entre claim, the Court is of the opinion that there is nothing confusing about this phrase. Specifically, the Court has already construed the phrases "authentication and encryption program," "server," and "generate a session key." In the light of these constructions, the entire phrase will be understandable to a jury whenever the construction of the individual terms is provided by the Court. The Court further finds that Defendants' proposed construction imports an artificial limitation by attempting to restrict the manner in which the claimed "session key" is "generated." For example, Defendants' proposal would limit the "generating" step to one in which "the first client computer produces

the session key through communications with the server." This limitation is not required by the claims or the patent specification. To be sure, the claim language itself recites that the session key is generated by the applications level authentication and encryption program. In addition, in discussing the SmartGATE™ system, the specification states that "it is of course within the scope of the invention to use key distribution and authentication methods which do not rely on smartcards or tokens, and the tokens are not involved in any of the basic communications functions of the client authentication software 20." '976 patent, 9:6-10. During the claim construction hearing, Defendants argued that its proposed construction attempted to capture the logical ordering of steps recited in the claims. As discussed above, the Court has addressed this concern by providing a high-level logical ordering of the steps. Accordingly, Defendants' proposed language is ambiguous and would not be helpful to the jury. Thus, the Court finds that no construction is necessary.

11. "recreate the session key"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
recreate the session key	generate the same session key (as another).	reproduce the same session key previously created

The Court construes "recreate the session key" as "recreate the sequence of bits that is input into an encryption algorithm to encrypt data for a session." The Court has adopted the parties' agreed construction for the phrase "session key" as "a sequence of bits that is input into an encryption algorithm to encrypt data for a session." Thus, the parties' dispute is focused on whether the term "recreate" means to "generate," as proposed by Plaintiff, or to "reproduce" as proposed by Defendants. The Court finds that in the context of the entire claim, the term "recreate" is not confusing and will easily be understood by a jury. Specifically, the disputed claim term reads "recreate *the* session key." The use of the definite article "the" requires that

"session key" have an antecedent basis, which is necessarily a session key referenced earlier in the claim steps. The antecedent basis for "recreate the session key" is the reference to the earlier generation of the session key (*i.e.*, "causing an applications level authentication and encryption program . . . to communicate with the server, generate *a session key*, and use the session key . . ."). Thus, the claim term here refers back to the *same* session key that was generated in the earlier claim terms.

In addition, as determined by the Court, certain steps of the claimed method must be performed before other steps. In this case, the Court determined that the step that includes the earlier generation of the session key must be performed prior to the step that recites the disputed phrase "recreate the session key." Given this, the term "recreate" assumes its plain and ordinary meaning and will not be confusing to a jury. Moreover, Plaintiff's argument that the term "recreate" is "interchangeable" with "generate" is unsupported by the intrinsic evidence, and ignores the fact that the patentees used the term "generate" with reference to the session key three separate times in claim 27 before the "recreation" step. Accordingly, the Court construes "recreate the session key" as "recreate the sequence of bits that is input into an encryption algorithm to encrypt data for a session"

12. "transmitting the encrypted files directly to the destination address"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
transmitting the encrypted files **directly** to the destination address	The term "directly" does not need to be construed and should be given its plain and ordinary meaning. However, if the Court determines that the term should be construed, the term "directly" as used in the phrase "transmitting the encrypted files directly to the destination address" means transmitting the encrypted files on a path to a destination address with or without intermediary points in-between. The terms "files" and "destination address" are discussed elsewhere in this chart.	Transmitting the encrypted files to the destination address without being relayed by a server

The Court construes "transmitting the encrypted files directly to the destination address" as "transmitting the encrypted files from a first client computer to a second client computer."

A. Parties' Construction Arguments

The parties dispute whether "directly" means "transmitting the encrypted files to the destination address without being relayed by a server," as proposed by Defendants. Defendants argue that their proposed construction comports with the plain language of the claim and the teachings of the specification. They further contend that Plaintiff's construction is wrong because it requires that the Court construe "directly" to mean "indirectly." Plaintiff argues that the "direct link" (62, Fig. 6) between end-points is a "tunnel" established through an open network such as the Internet. *See, e.g.*, 11:40-44. Plaintiff contends that any number of intermediate relay points (e.g., servers, routers, etc.) are known in the art to be used in passing traffic through the Internet. The reliance on such intermediate points is so prevalent and commonplace that they are popularly referred as a "cloud," which is illustrated (i.e., "cloud 8") in Figure 6. Plaintiff argues that such a cloud may be used for providing the "direct" connection

between VPN clients. Given this, the Court turns to the intrinsic evidence to determine how one of ordinary skill in the art would interpret this phrase.

B. Findings

To begin its analysis, the Court turns to the claims themselves. The phrase "transmitting the encrypted files directly to the destination address" appears in claim 27 of the '796 patent. In the context of the entire claim, the Court agrees that Defendants' proposed construction attempts to improperly narrow the claim. That is, Defendants' proposed construction imposes the restriction that no server could be used in effecting a "direct" communication. This is contrary to the intrinsic evidence. Instead, the Court finds that the direct communication is one between the client computers that does not require the recited server to actively transmit the encrypted files between the client computers. This, of course, does not mean that the direct transmission cannot pass through various mid-points, including receivers, transmitters, and other intermediary components, before arriving at the second of said client computers as indicated by "cloud" 8 in Figure 6. It only removes the recited server from its role as an active participant in establishing the initial connection, but it does not prevent the transmission from later passing through the recited server. Indeed, in describing Figure 6, the specification states that "[a]lternatively, after establishing channel 63, the channel 60 session key could be used to transmit back to the original sending party information necessary to recreate the channel 63 session key." '976 patent, 11:36-40. Likewise, the specification discloses that in peer-to-peer communications each client acts as its own "server." Thus, adopting Defendants' proposed construction would be inconsistent with the intrinsic evidence. Accordingly, the Court construes "transmitting the encrypted files directly to the destination address" as "transmitting the encrypted files from a first client computer to a second client computer."

13. "mutually authenticate the server and client computer initiating communications with the server"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
mutually authenticate the server and client computer initiating communications with the server	The term "mutually authenticate" does not need to be construed and should be given its plain and ordinary meaning. However, if the Court decides the term needs to be construed, "mutually authenticate the server and client computer initiating communications with the server" means the client computer performs an authentication function using information provided by the server and the server performs an authentication function using information provided by the client computer. The terms "server" and "client computer" are discussed elsewhere in this chart. The term "initiating communications" has not been identified as requiring construction.	The server verifies the identity of the client computer and the client computer verifies the identity of the server

The Court has construed the terms "server," "client computer," and "authentication." In addition, the parties have not suggested that the phrase "initiating communications" requires a construction. Thus, the only term remaining to be construed is the term "mutually," as in "mutually authenticate" as it is recited in claims in 2 and 4 of the '011 patent. Plaintiff contends that the term "mutually" has a generally accepted meaning well within the understanding of a jury. Defendants contend that the term "mutual" authentication is where two entities communicating on a network verify one another's identity. The Court has construed "authentication" to mean "verifying the identity of a client or server." The claims explicitly recite the two entities to be authenticated are the "client computer" and "the server." In addition, the '918 patent indicates that "mutual authentication" is a process in which two entities to a communication verify one another's identity. '918 patent, 4:32-42 & 5:1-29. Accordingly, the

Court construes "mutually authenticate" as "a server verifies the identity of the client computer and the client computer verifies the identity of the server."

14. "a shim"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
a shim	The claim term "a shim" is only found in claims 2 and 4 of the '011 patent. Therefore, any attempt to artificially write in the claim term "a shim" into the language of any other asserted claim should be rejected. "Shim" does not need to be construed and should be given its plain and ordinary meaning. However, if the Court determines that the term should be construed, "shim" means software introduced at a specific lower layer (or between layers) of a communications hierarchy on a computing device, where the software receives requests from a higher layer that are intended for other software at or below that specific lower layer.	Software that is added between two existing layers and which utilizes the same function calls so that the existing layers do not need to be modified. Software that only affects communications directed to an authentication server is not a shim

The Court construes "a shim" as "software that is added between two existing layers, which utilizes the same function calls of the existing layers."

A. Parties' Construction Arguments

The parties dispute whether the term "shim" needs to be construed. Plaintiff argues that that "a shim" is notoriously well-known in the art, and is simply software added to an existing operation to perform one or more specific functions. Defendants agree that the term "shim" is software and that this software is added between two existing layers of a computer system.

Thus, the dispute is whether the construction should include: (1) utilizing the same function calls so that the existing layers do not need to be modified; and (2) whether software that only affects communications directed to an authentication server would be considered a shim. Given this, the Court turns to the intrinsic evidence to determine how one of ordinary skill in the art would interpret this phrase.

B. Findings

To begin its analysis, the Court turns to the claims themselves. The term "shim" appears in asserted claims 2 and 4 of the '011 patent. The term also appears in a number of the claims not asserted in the '796 patent and the '011 patent. The Court concludes that the term is used consistently in each patent and is meant to have a similar meaning. Second, the claim language explicitly provides that a "shim" is software that is added between two existing layers. For example, claim 28 of '796 patent recites that the shim is "positioned between a peer-to-peer applications program and a layer of a communications driver architecture of said one of the two client computers." With this in mind, the Court turns to the specification and prosecution history for further insight.

Defendants contend that the term "shim" is expressly defined in the patent when it states:

> If possible, it is generally desirable to minimize modification of the existing levels by adding *a layer to perform the desired functions, calling upon the services of the layer below, while utilizing the same function calls so that the higher layer also does not need to be modified. Such a layer is commonly referred to as a "shim."*

3:60-66 (emphasis added). This portion of the specification confirms that the patent discloses that a shim is software added between two existing layers ("the higher layer" and "the layer below"). It also indicates that a shim utilizes the same function calls of the existing layers. *See also* Figs. 3-5 (depicting shims).

The Court finds that the prosecution history further informs the meaning of the term "shim." During prosecution of the '011 patent, the patentee defined "shim" in order to distinguish the claimed inventions from the prior art:

> [I]nstead of just providing a socket that provides encryption services as in the Elgamel patent, *the present invention inserts a shim between the sockets layer and applications programs* that use the sockets layer. The shim diverts function calls to an applications level encryption and authentication program…. There is *no need to modify either the sockets layer or the applications program* by adding new function calls as taught by Elgamel…

(Dkt. No. 101-19 at 75 (SSL0010157) (emphasis added).) Given this intrinsic evidence, the Court concludes that a "shim" is "software that is added between two existing layers, which utilizes the same function calls of the existing layers."

The Court does not agree, however, that the patentee unequivocally disavowed a certain meaning of the term by explaining what a shim is not. Specifically, Defendants appear to rely on the portion of the patent specification that describes the prior use of software referred to as SmartGATE™. '796 patent, 4:66-5:11. This passage, however, does not purport to define or provide any characteristic of a "shim," as used in the claimed invention. Instead, it simply provides additional background illustrating known software (i.e., the SmartGATE™ software) that was not "used" as a "shim" under the particular circumstances of that implementation. Thus, the Court finds that the patentee did not "disclaim" any claim scope of the term "shim" that would cover software that only affects communications directed to the authentication server. To be sure, neither the specification nor prosecution history shows a clear intention to limit the term "shim" as proposed by Defendants. *Liebel-Flarsheim v.Medrad, Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004). Accordingly, the Court construes "a shim" as "software that is added between two existing layers, which utilizes the same function calls of the existing layers."

15. "said function calls and requests for service being limited to communications functions without reference to encryption/ said intercepted function calls and requests for service being limited to communications functions without reference to encryption"

Claim Phrase	SSL's Proposed Construction	Citrix's Proposed Construction
said function calls and requests for service being limited to communications functions without reference to encryption/ said intercepted function calls and requests for service being limited to communications functions without reference to encryption	The phrase "communications functions without reference to encryption" does not need to be construed and should be given its plain and ordinary meaning. However, if the Court determines that the phrase should be construed, "communications functions without reference to encryption" means function calls and requests for service that do not explicitly reference an encryption protocol (e.g., secure sockets layer (SSL)). The clause "function calls and requests for service" is discussed elsewhere in this chart.	Ordinary, unmodified function calls and requests for service having no reference to encryption functions

After reviewing the disputed phrase in the context of the entre claim, the Court is of the opinion that there is nothing confusing about this phrase. The Court therefore finds that no construction is necessary. The parties' dispute centers on the meaning of "being limited to communications functions without reference to encryption." Defendants contend that the term means "ordinary, unmodified function calls and requests for service having no reference to encryption functions." Plaintiff argues that Defendants' proposed construction is an improper attempt to further limit the subset of claimed "function calls and requests for service" to those that are "ordinary" and "unmodified." Plaintiff argues that the claim phrase does not need any interpretation and terms comport with the widely accepted meaning of commonly understood

words. That is, the function calls and requests for service are without reference to encryption. The Court agrees and notes that it has already addressed the phrase "function calls and requests for service."

The Court also agrees that the patentee's statement made during the prosecution history of '011 patent was not to limit the claim scope as Defendants suggest with their proposed construction. Instead, it described one implementation of the claimed invention, showing how it differed from the prior art. (Dkt. No. 98-9 at 6 (Request for Reconsideration at 4).) That is, the patentee's intent to limit its claim scope was captured by the amendments to claims 1, 4 and 7, in which patentee expressly limited the applicable "function calls and requests for service" to those "without reference to encryption." Accordingly, given that the phrase "function calls and requests for service" has been addressed by the Court, the Court is of the opinion that there is nothing confusing about this disputed phrase. The Court therefore finds that no construction is necessary.

VI. CONCLUSION

The Court adopts the constructions set forth in this opinion for the disputed terms of the patents-in-suit. The parties are ordered that they may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the Court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the Court.

SIGNED this 20th day of September, 2011.

T. JOHN WARD
UNITED STATES DISTRICT JUDGE